MEND | MSCI

Mend Helps MSCI Address Spring4Shell in Hours

About The Company

MSCI is a leading provider of critical decision support tools and services for the global investment community. With over 50 years of expertise in research, data, and technology, MSCI powers better investment decisions by enabling clients to understand and analyze key drivers of risk and return and confidently build more effective portfolios. MSCI creates industry-leading research-enhanced solutions that clients use to gain insight into and improve transparency across the investment process.

Approximately half of their employees are involved in some way with either software development or IT operations, with a dedicated team responsible for application security.

The Challenge

Before the Spring4Shell announcement

In 2020, MSCI decided to adopt modern DevOps methodologies across all their business units to improve speed of application delivery, quality and reliability. Around the same time, the security team chose to standardize on Mend SCA for open source software security. By early 2022, Mend application security tools, including Mend SCA and Mend Renovate, were deployed across thousands of software projects spanning hundreds of repositories.

Chris Taylor, the Executive Director of Cyber Security at MSCI, knew that a good security program encompasses people, process and technology. He built MSCI's application security program on three main pillars:

- **People**: "You need empathy for what the developers' lives are like," Chris said. "We give our developers the information and the tools that they need to do their jobs, and we ensure that each DevOps team has a security SME. The goal should be familiarity, not mastery."
- **Process**: According to Chris, communication of software vulnerabilities has to take place at DevOps speed. To achieve that, MSCI integrated its Mend SCA with their Jira ticketing system. For the few development teams that are not using Jira, they're setting up Mend to trigger a daily email report.
- **Technology**: MSCI uses automation to trigger real-time testing with Mend SCA and Mend Renovate. This is designed to reduce friction and to "industrialize" the process as much as possible. According to Chris: "It is not reasonable to expect developers to constantly be working with separate security tools. So we try to make Mend as invisible as possible. Thanks to mend's various integrations and automations, we have been able to accomplish this."

The Mend Solution

Day Zero

On March 31, 2022, CVE-2022-22965, also known as the Spring4Shell vulnerability, was announced. This caused Mend SCA to send alerts via Jira or email to all software developers whose projects were impacted.

Chris explains: "For us, March 31 was not the emergency that Log4j was. We had refined our Zero Day processes just three months before, thanks to the Log4j drill. So everyone knew what to do. We had situational awareness within just a few hours. That was key! We knew which applications were priorities to address. Our IT staff applied mitigations to all the applications that needed them, and our developers were already working on applying the fixes."

Many MSCI developers relied on Mend Renovate to automate the pull requests to fix their vulnerable dependencies. Teams that had implemented automated testing did very well, whereas teams that were not as far along on their DevOps journey and had less automation took a bit longer.

> *"It is not reasonable to expect developers to constantly be working with separate security tools. So we try to make Mend as invisible as possible. Thanks to Mend's various integrations and automations, we have been able to accomplish this."*

The Results

According to Chris Taylor, "With Mend in place, and with the automation that we had designed, our developers and IT staff were able to turn everything around in a matter of hours. After that, it was just another day."

About Mend

Mend, formerly known as WhiteSource, effortlessly secures what developers create. Mend uniquely removes the burden of application security, allowing development teams to deliver quality, secure code, faster. With a proven track record of successfully meeting complex and large-scale application security needs, the world's most demanding software developers rely on Mend. The company has more than 1,000 customers, including 25 percent of the Fortune 100, and manages Renovate, the open- source automated dependency update project.

For more information, visit www.mend.io, the Mend blog, and Mend on LinkedIn and Twitter.